Verizon New England Inc
d/b/a Verizon Massachusetts

Commonwealth of Massachusetts

DTE 03-38

Respondent: Kathleen McLean
Title: Senior Vice President – Customer Relationship Management

REQUEST: Department of Telecommunications and Energy, Set #1

DATED: April 3, 2003

ITEM: DTE-VZ 1-1 Please refer to the Petition at 3, where Verizon states that "[a]t 1:00 AM EST Saturday, January 25, 2003, Verizon Network Management detected network flooding." Is network flooding the primary characteristic of a "worm" attack? Does Verizon identify 1:00 AM EST of January 25, 2003 as the beginning of the attack against the Verizon network?

REPLY: Network flooding was the primary characteristic of this worm. (In addition to creating garbage messages, other viruses and worms have attacked to consume or destroy the files, file structure, programs, operating systems or memory of individual computers.) According to industry reports, the worm attack began globally at 12:30 am EST on January 25, 2003. By 1:00 am, the Verizon Network Management team detected abnormally high levels of traffic on the Verizon computing network. This is indicative of the quick spreading nature of this worm.

Verizon New England Inc
d/b/a Verizon Massachusetts

Commonwealth of Massachusetts

DTE 03-38

Respondent: Kathleen McLean
Title: Senior Vice President – Customer Relationship Management

REQUEST: Department of Telecommunications and Energy, Set #1

DATED: April 3, 2003

ITEM: DTE-VZ 1-2 Please refer to the Petition at 3-5, where Verizon identifies the steps taken in response to the Slammer Worm. Verizon states that it detected network flooding at 1:00 a.m. on January 25, 2003. Verizon further states that "[l]ater that morning" its connections to the Internet were becoming flooded, and that it subsequently determined that an external quarantine process was necessary. When on the morning of January 25, 2003 did Verizon observe that its connections to the Internet were becoming flooded? At what time did Verizon "bring down" or disable the wholesale interfaces?

REPLY: See response to VZ 1-1. In addition, critical incident response began immediately with the technical teams seeking to determine the source of the attack, and taking defensive and remediation action. "Later that morning" refers to a time after 1 a.m., but before 11 a.m. Due to the circumstances, the exact time that Verizon observed that it connections to the Internet were becoming flooded was not recorded. At 11:23 am Verizon notified the CLECs that the interfaces would be brought down for emergency maintenance. The activities to disable the interfaces were concluded by 1:30 pm.

Verizon New England Inc
d/b/a Verizon Massachusetts

Commonwealth of Massachusetts

DTE 03-38

Respondent: Kathleen McLean
Title: Senior Vice President – Customer Relationship Management

REQUEST: Department of Telecommunications and Energy, Set #1

DATED: April 3, 2003

ITEM: DTE-VZ 1-3 Please refer to the Petition at 4, where Verizon indicates that it disabled the wholesale interfaces. When Verizon brought down the wholesale interfaces, did this action stop or mitigate the effect of the Slammer Worm? What was the nature of the damage sustained by Verizon due to the effects of the Slammer Worm?

REPLY: Shutting down the external interfaces to the VZ computing network mitigated the effect of the worm by stopping the external generation of spurious messages. The net effect of the worm was the temporary "clogging" of the computing network such that legitimate messages were extremely slow in being delivered. There was no long-term damage to the Verizon computing network.

Verizon New England Inc
d/b/a Verizon Massachusetts

Commonwealth of Massachusetts

DTE 03-38

Respondent: Kathleen McLean
Title: Senior Vice President – Customer Relationship Management

REQUEST: Department of Telecommunications and Energy, Set #1

DATED: April 3, 2003

ITEM: DTE-VZ 1-4 Please refer to the Petition at 4, where Verizon indicates that it disabled the wholesale interfaces. Did Verizon disable any other web access besides the wholesale interfaces? What other actions did Verizon take in response to the Slammer Worm?

REPLY: Verizon blocked the offending traffic on its connections to external networks, which included not only wholesale but also retail and administrative communications paths. This was part of the effort to defend and recover from the attack. Verizon isolated and quarantined the computing network into several segments, then proceeded to inspect, identify and remove infected devices and where appropriate patch, test and reconnect devices thus incrementally restoring segments of the computing network. Verizon also reported the attack to the National Communications Center – Information Sharing & Analysis Center (NCC-ISAC), an industry and government group established for the purposes of sharing information about such cyber attacks.

Verizon New England Inc
d/b/a Verizon Massachusetts

Commonwealth of Massachusetts

DTE 03-38

Respondent: Kathleen McLean
Title: Senior Vice President – Customer Relationship Management

REQUEST: Department of Telecommunications and Energy, Set #1

DATED: April 3, 2003

ITEM: DTE-VZ 1-5 Please refer to the Petition at 4, where Verizon states that it notified CLECs by email of "the event," and then later issued an updated bulletin via the standard email notification. Provide a copy of each of these notifications. Describe Verizon's "standard email notification" as it applies here.

REPLY: When an interface outage occurs, Verizon's Wholesale Customer Care Center (WCCC) sends an email notification to a distribution list of CLEC users. The WCCC issues a bulletin when the outage is detected or about to occur, and then issues a subsequent bulletin when the interface is to be restored. The WCCC outage bulletins are attached. See WCCC_EmgergencyMaintenance_012503_1023am.pdf and WCCC_EmgergencyMaintenance_012503_1000pm.pdf.

Verizon New England Inc
d/b/a Verizon Massachusetts

Commonwealth of Massachusetts

DTE 03-38

Respondent: Kathleen McLean
Title: Senior Vice President – Customer Relationship Management

REQUEST: Department of Telecommunications and Energy, Set #1

DATED: April 3, 2003

ITEM: DTE-VZ 1-6 Please refer to the Petition at 4. In the early morning of January 25, 2003, were CLECs negatively affected by the network flooding experienced by Verizon before the wholesale interfaces became unavailable, or were CLECs affected only after the wholesale interfaces were disabled?

REPLY: Only one CLEC notified Verizon that it was experiencing difficulty using a Verizon interface as a result of the network flooding caused by the worm. That CLEC indicated, at 7:30 am, that it was experiencing slow response time using the web-based interface, LSI. January 25th was a Saturday and although designated as "prime time" for availability metrics calculation purposes, Saturdays are historically low volume days, so other than this one CLEC, it does not appear that other CLECs were adversely affected in attempting to use Verizon interfaces.

It is important to note however, that the CLECs' systems themselves likely were directly affected by the worm. Press reports and information Verizon garnered through operational contacts indicated that to the extent the systems of CLECs relied on Microsoft's SQL Server 2000 and shared Internet-attached networks, they too were dealing with the fallout of the Slammer Worm on and after January 25, 2003.

Verizon New England Inc
d/b/a Verizon Massachusetts

Commonwealth of Massachusetts

DTE 03-38

Respondent: Kathleen McLean
Title: Senior Vice President – Customer Relationship Management

REQUEST: Department of Telecommunications and Energy, Set #1

DATED: April 3, 2003

ITEM: DTE-VZ 1-7 When the wholesale interfaces became unavailable on the morning of January 25, 2003, what alternative methods existed for CLECs to continue to communicate and do business with Verizon? Were these alternatives adequate for CLECs to continue to interface with Verizon to perform wholesale functions?

REPLY: CLECs needing to open repair trouble tickets were able to call the Regional CLEC Maintenance Center (RCMC), and CLECs with system issues were able to call the Wholesale Customer Care Center (WCCC), which is the standard operating practice on Saturdays. January 25, 2003, was a Saturday and the other wholesale centers are not open on Saturdays. Verizon's wholesale web site contains contact information for out of hours escalations. In addition, orders that are received over weekends and holidays that require manual handling are processed on the next business day.

Furthermore, as noted in DTE-VZ 1-6, the CLECs that rely on Microsoft's SQL Server 2000 and shared Internet-attached networks were also dealing with the fallout of the Slammer Worm on and after January 25, 2003 and may have been incapable of interfacing with Verizon.

Finally, Verizon's performance is not evaluated on an incident basis. Instead, its performance is measured under the various standards and time frames in the PAP. A review of the numerous pre-order,

REPLY: DTE-VZ 1-7 (cont'd) provisioning and maintenance metrics included in the January 2003 PAP monthly report demonstrates that Verizon provided CLECs with exceptional service. In particular, Verizon provided excellent service on the fifteen (15) PO-1 "Response Time OSS Pre-Ordering Interface" submetrics that are included in the PAP.

VZ # 7

Verizon New England Inc
d/b/a Verizon Massachusetts

Commonwealth of Massachusetts

DTE 03-38

Respondent: Kathleen McLean
Title: Senior Vice President – Customer Relationship Management

REQUEST: Department of Telecommunications and Energy, Set #1

DATED: April 3, 2003

ITEM: DTE-VZ 1-8 Please refer to the Petition at 2, where Verizon states "[o]ne industry report estimates that 'more than 90 percent of vulnerable computers [were infected] within 10 minutes.'" Explain what is meant by the phrase "vulnerable computers" in the above quote. What is the reason that ten percent of "vulnerable computers" were not susceptible, whether sooner or later? Did the source document identify functions and/or facilities that were resistant to the Slammer Worm? If yes, state what they were, and why they were not vulnerable. Provide a copy of the source document ("Week in Review: Worm's Wrath" in CNET News.com of Feb. 7, 2003).

REPLY: Although Verizon did not author the article, our understanding is that in this situation a "vulnerable computer" was a computer that was running a version of MS SQL Server 2000 or Microsoft Desktop Engine (MSDE) 2000 which contained a specific defect and was connected directly or indirectly to the Internet or an Internet-attached network. All vulnerable computers were *susceptible* to the worm, but not all vulnerable computers were actually *infected* within the first 10 minutes. Some of that remaining 10 percent were infected later as the worm continued to rapidly spread across the globe, and some were not infected at all because they were removed from the Internet-attached network or the connection to the Internet was disabled or blocked before it could be infected. After the attack, the defect that was exploited by the worm was described in various industry forums as was

REPLY: DTE-VZ 1-8 (cont'd)

the "patch" or code fix that was needed to plug the security hole. Computers running MS SQL Server 2000 or MSDE 2000 that had the patch applied were not vulnerable.
Attached is a copy of "Week in Review: Worm's Wrath".

VZ # 8

Verizon New England Inc
d/b/a Verizon Massachusetts

Commonwealth of Massachusetts

DTE 03-38

Respondent: Kathleen McLean
Title: Senior Vice President – Customer Relationship Management

REQUEST: Department of Telecommunications and Energy, Set #1

DATED: April 3, 2003

ITEM: DTE-VZ 1-9 Please refer to the Petition at 3, where Verizon states "[t]he Slammer Worm hit the national (and international) network quickly and without warning." If there is warning of a "worm" attack, name the entities that would furnish Verizon with such a warning. Indicate whether the warnings estimate likelihood of attack, timing of its onset, and the potential severity. If Verizon has warning of a "worm" attack, outline the sequence of preparations that it follows in order to guard itself. Identify when, and by what means, did a warning about the Slammer Worm reach Verizon?

REPLY: Verizon is vigilant in protecting the security of its physical and cyber assets. Its security practices have repudiated countless cyber attacks. Among the security practices employed by Verizon is participation in industry and government security information-sharing forums such as the NCC-ISAC and the Computer Emergency Response Team ("CERT") Coordination Center at Carnegie Mellon University. Verizon also has engaged the services of a third-party firm specializing in software security, which proactively notifies Verizon of impending cyber attacks. None of these external groups provided Verizon advanced warning of the Slammer Worm. In fact, Verizon was the first telecommunications company to notify the NCC-ISAC once the attack began. (In contrast to other famous virus incidents, Verizon had one day's notice before the CodeRed attack and 3 days notice before the Nimda attack.) If Verizon had had advance notice of the attack, it would have taken the same steps it took to recover from the attack, the only difference would have been in the timing (i.e., proactively versus reactively). These steps include, identifying vulnerable computers, removing them from the network, applying and testing the patch

REPLY: DTE-VZ 1-9
(cont'd) and reattaching the computers to the network.

Verizon New England Inc
d/b/a Verizon Massachusetts

Commonwealth of Massachusetts

DTE 03-38

Respondent: Kathleen McLean
Title: Senior Vice President – Customer Relationship Management

REQUEST: Department of Telecommunications and Energy, Set #1

DATED: April 3, 2003

ITEM: DTE-VZ 1-10 Please provide a copy of Verizon's policy for responding to computer virus/worm infections. Was this policy followed on January 25-26, 2003? If not, why not?

REPLY: The requested information is Proprietary as the information is related to the security of Verizon's network. Therefore, the requested information is being provided only to the Department. Verizon acted in a manner consistent with the appropriate policy guidelines. See also response to DTE-VZ 1-14.

VZ # 10

Verizon New England Inc
d/b/a Verizon Massachusetts

Commonwealth of Massachusetts

DTE 03-38

Respondent: Kathleen McLean
Title: Senior Vice President – Customer Relationship Management

REQUEST: Department of Telecommunications and Energy, Set #1

DATED: April 3, 2003

ITEM: DTE-VZ 1-11 Please provide a copy of Verizon's computer security practices identifying the steps Verizon takes to protect itself from computer viruses/worms such as the Slammer Worm. Were these practices followed during the Slammer Worm incident? If not, why not?

REPLY: See responses to VZ 1-10 and 1-14. The Company's computer security practices are contained in Verizon Information Security Corporate Policy-Instruction that document contains information related to computer security and will be made available for the Department's inspection at a Company location at a mutually agreeable time. Verizon acted in a manner consistent with its policies in this area, however, as reported in the press and known throughout the industry, it is impossible for a large-scale computing infrastructure to be "100% patched" at any given time.

Verizon New England Inc
d/b/a Verizon Massachusetts

Commonwealth of Massachusetts

DTE 03-38

Respondent: Kathleen McLean
Title: Senior Vice President – Customer Relationship Management

REQUEST: Department of Telecommunications and Energy, Set #1

DATED: April 3, 2003

ITEM: DTE-VZ 1-12 Please refer to the Petition at 3, where Verizon references the Network and Information Security teams. Describe the purpose and capabilities of Verizon Network and Information Security. Is it the group that has responsibility for dealing with problems like"worms"? If not, identify the group that has responsibility.

REPLY: The Network security team has responsibility to establish, maintain and enforce security rules, procedures and instructions for connectivity and use of the internal Verizon network. Responsibilities include intrusion detection and response. The Information Security team is responsible for the management of information security including firewall support, computer management, virus protection, risk assurance, information security practices and awareness, incident response and vulnerability scanning, and remote access security administration. These responsibilities include the evaluation, approval and installation of security patches to the various third-party software products across multiple systems and platforms used in the Verizon computing infrastructure. Patch management is a complex and time-consuming function for large information technology organizations such as Verizon, the computing network of which contains over 233,000 addressable devices. The Information Security group evaluates the thousands of patches that are announced annually by Verizon's software vendors and works with the various application teams to schedule and install security upgrades. In addition, each Verizon

REPLY: DTE-VZ 1-12 (cont'd) employee is responsible for adherences to the Verizon Code of Conduct, which includes the safeguarding the confidentiality and integrity of our corporate systems.

Verizon New England Inc
d/b/a Verizon Massachusetts

Commonwealth of Massachusetts

DTE 03-38

Respondent: Kathleen McLean
Title: Senior Vice President – Customer Relationship Management

REQUEST: Department of Telecommunications and Energy, Set #1

DATED: April 3, 2003

ITEM: DTE-VZ 1-13 Does Microsoft offer assistance in fighting "worms" to its customers? If the answer is yes, what kinds of assistance does Microsoft offer? Did Verizon, in dealing with the Slammer Worm, seek the assistance of Microsoft? If so, what type of assistance did Microsoft provide?

REPLY: Microsoft has a technical support section in its web site. Verizon regularly reviews the web site to obtain information about software defects and available repairs (also known as patches) for the various Microsoft products and versions in use in the Verizon computing infrastructure. On the day of the attack, contacting Microsoft was difficult due to the Internet flooding and the fact that Microsoft itself had been infected by the worm.

Verizon New England Inc
d/b/a Verizon Massachusetts

Commonwealth of Massachusetts

DTE 03-38

Respondent: Kathleen McLean
Title: Senior Vice President – Customer Relationship Management

REQUEST: Department of Telecommunications and Energy, Set #1

DATED: April 3, 2003

ITEM: DTE-VZ 1-14 Please refer to the Petition at 6-7, where Verizon discusses patch management. Provide a copy of Verizon's patch management policy. Are patches identified by level of importance or priority? Does Verizon' patch management policy address patches differently depending on the priority of a patch? Did Verizon follow its patch management policy with regard to patches that address the vulnerabilities exploited by the Slammer Worm? If not, why not?

REPLY: See also VZ 1-10 and 1-11. Generally speaking, the software vendor will designate the level of importance of a patch, which Verizon will then take into account when assessing its level of criticality with respect to its computing infrastructure. Verizon acted in a manner consistent with its policies in addressing the Slammer Worm. See also response to VZ 1-15.

Verizon New England Inc
d/b/a Verizon Massachusetts

Commonwealth of Massachusetts

DTE 03-38

Respondent: Kathleen McLean
Title: Senior Vice President – Customer Relationship Management

REQUEST: Department of Telecommunications and Energy, Set #1

DATED: April 3, 2003

ITEM: DTE-VZ 1-15 Refer to the Petition at 7-8, where Verizon references a patch or patches to "fend off the Slammer Worm." Verizon also states that Microsoft "had released security patches that addressed the specific vulnerability exploited by the Slammer Worm." When did Microsoft issue a patch for the Slammer Worm? Had Verizon received a specific patch or patches to protect against the effects of computer infections such as the Slammer Worm? When did Verizon become aware of this patch? How was Verizon notified of the patch? When did Verizon receive this patch? Was this patch installed, and to what extent was it installed, before January 25, 2003? Was this patch identified by a particular priority rating? If this patch was not installed before January 25, 2003, why was this particular patch not installed? If such a patch was utilized, how did it perform in the Verizon network?

REPLY: See response to VZ 1-14. Verizon, Microsoft, CERT and other industry members were aware of several security vulnerabilities in MS SQL Server 2000. In this particular part of Microsoft's code, there were three known buffer overflow vulnerabilities and one weak permissions vulnerability about which Verizon and others were aware. In July 2002, Microsoft released a "standalone" patch, designated as "critical" that addressed one of the buffer overflow vulnerabilities. That patch from Microsoft left the other two buffer overflow vulnerabilities open and the permission vulnerability open. However,

REPLY: DTE-VZ 1-15 (cont'd)

the Service Pack, which fixed a number of defects including these, and which included the tools typically appropriate for patch installation, was not released until almost six months later on January 17, 2003 in Microsoft's Service Pack 3 (SP3). Verizon had obtained SP3 and was in the process of evaluation and testing when the Slammer Worm struck on January 25, 2003. This patch was identified as a critical patch. (Of the 72 security patches released by Microsoft in 2002, 35 were designated as critical.) It had been installed on some Verizon devices before January 25, 2003, but as stated by Microsoft when discussing its own experience, "it only took one machine to get it going."

Verizon New England Inc
d/b/a Verizon Massachusetts

Commonwealth of Massachusetts

DTE 03-38

Respondent: Kathleen McLean
Title: Senior Vice President – Customer Relationship Management

REQUEST: Department of Telecommunications and Energy, Set #1

DATED: April 3, 2003

ITEM: DTE-VZ 1-16 Please refer to the Petition at 8, where Verizon states that Microsoft has released new patches for the Slammer Worm. Has Verizon installed these new patches? If not, why has Verizon declined to install these particular patches?

REPLY: To recover from the Slammer attack, Verizon identified the devices needing the patch, isolated them, installed and tested the patch, then reattached the devices to the network.

Verizon New England Inc
d/b/a Verizon Massachusetts

Commonwealth of Massachusetts

DTE 03-38

Respondent: Kathleen McLean
Title: Senior Vice President – Customer Relationship Management

REQUEST: Department of Telecommunications and Energy, Set #1

DATED: April 3, 2003

ITEM: DTE-VZ 1-17 In response to its experience with the Slammer Worm, describe changes that Verizon has implemented, or considers implementing, in order to maintain network performance. Include changes in policies and procedures, as may be applicable.

REPLY: Verizon continues to review and evaluate these policies. Verizon has distributed several security bulletins to employees to heighten their awareness and remind them about their roles and responsibilities in protecting Verizon's assets.

VZ # 17